

[Insert Picture of Your Facility]

Faith-Based Organizations Tabletop Exercise

Situation Manual

[Insert Date]

[Insert Caveat]



CISA Tabletop Exercise Package (CTEP) Faith-Based Organizations Tabletop Exercise Situation Manual (SitMan)

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

EXERCISE AGENDA

Time	Activity
0815 - 0900	Registration
0900 - 0915	Welcome and Participant Briefing
0915 - 1015	Module One - Threat
1015 - 1030	Break
1030 - 1130	Module Two - Incident
1130 - 1200	Hot Wash

**All times are approximate*

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Faith-Based Organizations Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX planned for [insert exercise duration] at [insert exercise location]. Exercise play is limited to [insert exercise parameters]. This exercise was developed using materials created by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Areas]
Core Capabilities	Planning; Intelligence and Information Sharing; Risk Management for Protection Programs and Activities; and, Public Information and Warning
Objectives	1. Review intelligence and information sharing and dissemination processes in relation to a credible threat to Faith-Based Organizations (FBOs). 2. Discuss emergency preparedness plans and public messaging procedures to a threat-initiated incident. 3. [Insert additional exercise objectives as necessary.]
Threat or Hazard	Active Shooter and Improvised Explosive Device (IED) (international threat and domestic attack).
Scenario	An interactive, discussion-based exercise focused on an international and domestic active shooter and IED attack. The scenario consists of two modules: Threat, and Incident.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]
Participatin	[Insert a brief summary of the total number of



**g
Organizations**

participants and participation level (i.e., Federal, State, local, tribal, non-governmental organizations [NGOs], private sector, and/or international agencies). Consider including the full list of participating agencies in Appendix A. Delete Appendix A if not required.]

**Points of
Contact**

[Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (e.g., exercise director or exercise sponsor)]

GENERAL INFORMATION

Exercise Objectives and Core Capabilities

The exercise objectives listed in Table 1 describe the expected outcomes from the TTX. These objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific prevention, protection, and response mission areas. The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objective	Core Capability
Review intelligence and information sharing and dissemination processes in relation to a credible threat to FBOs.	✓ Planning ✓ Intelligence and Information Sharing ✓ Risk Management for Protection Programs and Activities
Discuss emergency preparedness plans and public messaging procedures to a threat-initiated incident.	✓ Planning ✓ Risk Management for Protection Programs and Activities ✓ Public Information & Warning
[Insert additional objectives as necessary].	✓ [Insert additional core capabilities as necessary].

Table 1.—Exercise Objectives and Associated Core Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Types of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players.** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers.** Observers do not directly participate in the exercise; however, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also

assist with facilitation as subject matter experts (SMEs) during the exercise.

- **Evaluators.** Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

The TTX is comprised of two modules consisting of an overseas threat and domestic threats / incidents. Players in this exercise will participate in the following exercise module elements:

- Module One: Threat
- Module Two: Incident

Each module begins with a scenario update that summarizes the key events occurring within that time period. A series of questions following the scenario summary will guide the facilitated discussion of critical issues in each of the modules. Based on exercise priorities, time dedicated to each module will be managed by the facilitator.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- The situation updates, written material, and resources provided are the basis for discussion. There are no hidden materials or scenarios.
- Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, and response efforts. Problem-solving efforts should be the focus.

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to

negatively affect their participation. During this exercise, the following apply:

- The scenario for this exercise is fictitious and does not represent any actual intelligence.
- The scenario is plausible, and events occur as they are presented.
- There are neither “hidden agendas” nor any “trick questions.”
- All players receive information at the same time.
- Assume cooperation and support from other responders, agencies, and organizational entities.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the After-Action Report (AAR).

This page is intentionally left blank.

MODULE ONE: THREAT

Date: [Insert Incident Date - Two Weeks]

Amsterdam, Netherlands

10:00 a.m.: Two individuals exit the Gemeentelijk Vervoerbedrijf Tram at the A.J. Ernstraatstop in the vicinity of Vrije Universiteit. They continue on foot one block west on Arent Janszoon Ernststraat. One of the individuals proceeds on foot to the [insert a similar Faith-Based Organization to your own] of Amsterdam while the other waits at the bus stop. Approximately three minutes later, the second individual proceeds in the direction of the [insert the previous location].

10:09 a.m.: The first individual enters the building wearing a suicide vest concealed under a loose fitting shirt and light jacket and proceeds to the where the congregants are gathered. The vest is composed of Semtex and ball bearings. Once in the room, the first operative detonates his device and the blast and shrapnel instantly kill 12 people and injure another 20.

10:12 a.m.: Bystanders and the uninjured attempt to render first aid to victims and assist with evacuating the building. The second individual arrives outside the community center, as curious onlookers gather outside of the building. He is armed with a handgun and an AK-style rifle with a folding stock concealed in a backpack. He removes the rifle from the backpack and begins firing at the injured and those providing aid. An additional eight people are killed and 12 wounded outside of the center.

10:14 a.m.: Law enforcement and first responders arrive. Law enforcement officers briefly exchange gunfire with the second attacker, who is shot and killed while attempting to enter the building.

11:00 p.m.: Local police confirm the current toll is 20 killed and 32 injured.

Date: [Insert Incident Date - 13 Days]

There is still no claim of responsibility for the attack. Press reports indicate that law enforcement efforts to establish the identities of the attackers have been unsuccessful.

Discussion Questions

1. What is the process by which your organization would receive intelligence and protective measure information given an overseas threat?
 - A. What organizations would you communicate with (e.g., local law enforcement agencies, your Joint Terrorism Task Force [JTTF], Federal Bureau of Investigation [FBI])?

- B. Does your organization maintain a relationship with your DHS Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
- C. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI)?
- D. How does your organization triage the information you receive (e.g., formal reporting, rumors, social media) for further dissemination within your organization and to your staff and congregants?
 - I. Given current information sharing procedures, what types of official information are the most useful (immediate information versus analyzed information) to your organization?
 - II. Does your organization perform independent analysis on information provided and, if so, describe the process?
- 2. What information sharing and dissemination processes does your organization currently have in place to alert your staff and your congregants?
 - A. What notification capabilities (e.g., alerts, email, telecom, text message, special tools) do you use to share information and communicate protective measures implementation?
 - B. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?
 - I. If so, how will threat-based alerts and notifications be distributed to community members who follow religious customs that prohibit use of electronic communication during specific times?
- 3. In the event that your organization receives information related to potential threats against your facilities and personnel, how would you communicate this information to appropriate entities (local law enforcement agencies, your JTTF, FBI, your DHS PSA, etc.)?
- 4. If there is identified “suspicious behavior” observed at one your organization’s locations, how does the staff report this information to law enforcement officials and other members of your organization?
 - A. Are trends of suspicious behaviors tracked across your faith on a nation level?
 - B. Is your organization aware of the “If You See Something, Say Something™” campaign or the National Suspicious Activity Reporting (SAR) Initiative?

5. Given evidence of a credible threat to the facilities or people in your faith, what protective security measures or recommendations, if any, will be employed at your organization following this international attack?
- A. Does your organization review your emergency response plans (e.g., Site Security Plans, Emergency Occupancy Plans, Emergency Actions Plans, or other appropriate plans)?
 - B. Do you coordinate protective measure implementation with any other organization within your faith?
 - C. Do you coordinate protective measure implementation with government entities, such as law enforcement agencies and your DHS PSA?
 - D. Are you aware of the information bulletins and advisories DHS provides (e.g., a Joint Intelligence Bulletin [JIB]) that recommend protective measures?

MODULE TWO: INCIDENT

Date: [Insert date]

[Insert city name]

10:06 a.m.: Three individuals park near the [insert city] [insert your FBO's Facility]. The three men exit the vehicle, and one walks toward the building entrance, while the other two individuals remain on the sidewalk roughly 100 meters from the front door.

10:09 a.m.: The individual who entered the building shoots three people in the front lobby and continues down the hallway to the childcare area. The man detonates his suicide vest there (later determined to be comprised of 25 pounds of explosives, as well as an assortment of screws and bolts). With the attack begun, one of the two remaining attackers begins to roam the parking lot shooting at people with his AR-15 style rifle, while the second person targets people fleeing the building with his rifle. As law enforcement officers arrive the assailants target them, and gunfire is exchanged. During the brief firefight, the assailants are neutralized, and two officers are injured. Fire and Emergency Medical Service personnel stage nearby while this is occurring.

10:20 a.m.: After the attackers are neutralized, law enforcement officers work to clear the scene and then call in Fire and Emergency Medical service personnel. As a result of the attack, 32 people are killed and 45 more are injured.

[Insert the name of the secondary attack city or community]

12:10 p.m.: In [insert city], the [insert FBO school name] is abnormally busy for this time of day. As news of the [insert first location name] attack starts being reported on national news outlets, many concerned parents have gone to pick their children up from school early, and people are worried about visiting other places in their community.

12:15 p.m.: A man wearing business attire and carrying a briefcase makes his way towards the [insert FBO school name] entrance. The briefcase is filled with explosives (later estimated to be 30 pounds). A large group has gathered in front of the building as parents wait for their children to come out. The man places the briefcase by the front door and pulls out his cell phone as he walks back through the crowd and the parking lot.

12:17 p.m.: The man triggers the IED through his cell phone and it detonates. 31 people, including 11 children, are killed. An additional 16 people receive significant injuries.

1:30 p.m.: A local news station in [insert city] receives a posting on their Facebook wall stating, “We are everywhere and [insert name of adherents of the faith] will feel our presence.”

Discussion Questions

1. Do facility incident response plans (e.g. Site Security Plans, Emergency Action Plans, Emergency Response Plans, or other appropriate plans) contain protocol for responding to an Active Shooter / IED event?
 - a. Is staff trained for this type of emergency incident?
 - i. Is emergency contact information made available to the call desk?
 - ii. Are procedures in place for sheltering-in-place versus evacuation?
 - b. Do you have notification systems in place to warn staff and congregants both onsite and offsite during such an incident?
 - c. Is there a way to account for staff (i.e., those who reported for work that day versus those on leave)?
 - d. What does the facility emergency coordinator need to consider (e.g., injuries, evacuation routes, hospitals)?
 - e. What other life safety issues should be considered?
2. Is there security onsite at your facility?
 - a. How is security trained to respond to this type of incident? What are their roles and responsibilities?
 - b. Do security personnel and first responders have interoperable radios / communication? Are plans in place for agencies to communicate if they cannot communicate via radio?
 - c. Is security clearly identifiable upon arrival of law enforcement?
3. Does this facility have physical security measures that may be relevant to this scenario?
 - a. Is there any type of perimeter security (e.g., fences, doors, gates)?
 - b. What types of vehicle control checkpoints are present (e.g., barriers, driveways, parking lots)?
 - c. Does the public have access to the facility?
4. How is the emergency response coordinated?
 - a. Are any of the facility’s incident response plans provided to first responders in preparation for potential incidents?

- i. If not, how is the key information communicated to them during the response to an incident?
 - b. If there are locked doors, or other physical barriers, how do emergency response personnel access the buildings?
 - i. Upon arrival of law enforcement, is there a “go bag” available to them containing desired items such as facility map / floor plans, access swipe cards, elevator keys, etc.?
 - c. Are there any safety or religious concerns for first responders that need to be addressed (e.g., entering restricted, hazardous, or religiously sensitive areas)?
 - d. Have local first responders participated in exercises and/or training at your facility?
 - e. Do you know the specific local law enforcement policies and procedures regarding active shooter incidents for your location?
 - f. How is response coordinated and who maintains decision-making authority if management is not available?
 - i. Is delegation of authority captured in the security plan or any other plan?
 - g. Is there a safe location identified for people who are evacuating the immediate area?
5. How are communications related to the emergency handled?
 - A. Who is in charge of ensuring that staff and congregants are informed of the status of events?
 - B. What are your organization’s information sharing responsibilities during the response to the incident?
 - C. At what point do you begin sharing information with other members of your Faith-Based Organization?
 - d. How will your organization interact with media representatives and control media access to the facility?
 - e. Are there procedures in place to manage the media when they arrive?
 - f. Should additional emergency announcements be made to the public?
6. How do state and local officials coordinate to respond to an incident at the facility?
 - a. Do you have Memorandums of Understanding or Memorandums of Agreement in place with any local, regional, or state response agencies?

- b. What incident response plans do local, county, and state law agencies have in place for an active shooter / IED situation? Who leads the response?
 - c. What would state and local officials need from your organization during an incident similar to that detailed in this module?
7. Following the incident, what measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased vigilance, etc.)?
8. What assistance is available for staff and congregants following this event?
 - a. How is information communicated during the days following the incident?
 - b. Will counseling for members of your faith be available?
 - c. Will there be any financial assistance or benefit programs for staff if the facility is shut down on a temporary basis?
 - d. What is the procedure if a staff member is hospitalized by injuries received on the job (in this during the attack)?
9. Do the facility's incident response plans adequately address the emergency response and coordination activities described in the module? If not, what can be improved?

This page is intentionally left blank.



APPENDIX A: EXERCISE PARTICIPANTS

Participating Private Sector Organizations

[Insert private sector participants]

Participating Local Organizations

[Insert local participants]

Participating State Organizations

[Insert state participants]

Participating Federal Organizations

[Insert federal participants]

Other Participating Organizations

[Insert other participants]

This page is intentionally left blank.

APPENDIX B: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX C: ACRONYMS

Acronym	Definition
AAR	After-Action Report
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FBO	Faith-Based Organization
HSIN-CI	Homeland Security Information Network - Critical Infrastructure
IED	Improvised Explosive Device
JIB	Joint Intelligence Bulletin
JTTF	Joint Terrorism Task Force
NGO	Non-Governmental Organization
PSA	Protective Security Advisor
SAR	Suspicious Activity Reporting
SitMan	Situation Manual
SME	Subject Matter Expert
TTX	Tabletop Exercise